

**DIAMOND STATE PORT CORPORATION**

**JUNE 30, 2007**

**REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING  
AND ON COMPLIANCE AND OTHER MATTERS BASED ON  
AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN  
ACCORDANCE WITH GOVERNMENT AUDITING STANDARDS**

## REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH *GOVERNMENT AUDITING STANDARDS*

To the Board of Directors and Management  
of the Diamond State Port Corporation

We have audited the financial statements of the Diamond State Port Corporation as of and for the year ended June 30, 2007 and have issued our report thereon dated August 20, 2007. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

### Internal Control Over Financial Reporting

In planning and performing our audit, we considered the Diamond State Port Corporation's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Diamond State Port Corporation's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Diamond State Port Corporation's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceeding paragraph and would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the Diamond State Port Corporation's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the Diamond State Port Corporation's financial statements that is more than inconsequential will not be prevented or detected by the Diamond State Port Corporation's internal control. We consider the deficiencies described in the accompanying schedule of findings and responses, #1 and #2 described below, to be significant deficiencies in internal control over financial reporting.

Thomas John Shopa, CPA, CFP, CVA  
Charles H. Elter, CPA, CFP  
Robert S. Smith, CPA  
Ronald E. Derr, CPA  
George G. Fournaris, CPA, CGFM

■ Donald S. Emenheiser, CPA, CFP, MBA  
Edward T. Gallagher, CPA, CIA  
Dana L. Ketterer, CPA  
Clyde G. Hartman, CPA/ABV, CFE, CVA  
Cameron B. McDonald, CPA, CCIFP  
Jean D. Lloyd, CPA  
Scott G. Sipple, Jr., CPA  
Stuart A. Solomon, CPA (NJ)  
Alison L. Houck, CPA

Members of:  
American Institute of CPA's  
Private Companies Practice Section  
Delaware Society of CPA's

Certified Public Accountants  
A Professional Association

270 Presidential Drive  
Wilmington, DE 19807  
(302) 656-5500  
(302) 656-8024 Fax

37212 Rehoboth Avenue Ext.  
Rehoboth Beach, DE 19971  
(302) 227-4872  
(302) 227-4873 Fax

www.mcbrideshopa.com



An Independent Member of the BDO Seidman Alliance

REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING  
AND ON COMPLIANCE AND OTHER MATTERS BASED ON  
AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN  
ACCORDANCE WITH *GOVERNMENT AUDITING STANDARDS*  
(Continued)

To the Board of Directors and Management  
of the Diamond State Port Corporation  
Page 2

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the Diamond State Port Corporation's internal control.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Diamond State Port Corporation's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

We noted two other matters involving the internal control and its operation that we have reported to management of the Diamond State Port Corporation in a separate management letter dated August 20, 2007.

The Diamond State Port Corporation's response to the findings identified in our audit is described in the accompanying schedule of findings and responses. We did not audit the Diamond State Port Corporation's response, and, accordingly, we express no opinion on it.

This report is intended solely for the information and use of management, the Board of Directors of the Diamond State Port Corporation, the Office of Auditor of Accounts and others within the organization, and is not intended to be and should not be used by anyone other than these specified parties.

Sincerely,

*McBride, Shopa & Co*

August 20, 2007

DIAMOND STATE PORT CORPORATION  
SCHEDULE OF FINDINGS AND RESPONSES  
FOR THE YEAR ENDED JUNE 30, 2007

**SIGNIFICANT DEFICIENCY #1**

**INFORMATION TECHNOLOGY –  
PROGRAM CHANGE CONTROLS**

**Criteria:**

Best security practices require that programmers' access to the live production environment be restricted to prevent the posting of unapproved changes in program code.

**Condition:**

During our inquiries regarding general computer controls, we noted that programmers have access to post program changes to the live production environment without approval. The standard helpdesk process for program changes initiated by other departments involves IT management oversight and approval at all steps of the program change process. However, programmers have the ability to bypass this process and post potentially erroneous or malicious code directly to the live production environment without approval. As a compensating control, all program changes are logged and an individual responsible for any unauthorized change could be identified. However the program change log is voluminous and is not reviewed by IT management.

**Cause of Condition:**

Programmers have access to the live production environment.

**Effect of Condition:**

Programmers could potentially post unapproved program code directly to the live production environment.

**Recommendation:**

Remove programmer access to post program changes to the production environment. Programmers should only have access to post program changes to a test environment. The IT director who approves program changes should be the only individual with access to move program changes from the test environment to the production environment.

DIAMOND STATE PORT CORPORATION  
SCHEDULE OF FINDINGS AND RESPONSES  
FOR THE YEAR ENDED JUNE 30, 2007  
(Continued)

**Costs and Benefits of Recommended Action:**

Removing programmer access to the production environment may make the process of posting program changes slightly less efficient because departments will have to wait for IT Management to post the code themselves. However, the benefits of having control over the programming code in the production environment outweigh the cost.

**Client Response:**

On August 13, 2007, Inigo Thomas, IT Director, notified us that access to the production environment was removed for programmers. The issue has been satisfactorily resolved.

**SIGNIFICANT DEFICIENCY #2**

**INFORMATION TECHNOLOGY AND OTHER DEPARTMENTS –  
DISASTER RECOVERY & BUSINESS CONTINUITY PLANS**

**Criteria:**

Disaster recovery and business continuity planning for Information Technology are very important elements of General Control. Best practices require that, in an emergency, data processing continue to be performed. In addition to the recovery of IT resources, comprehensive contingency planning should incorporate all critical business requirements for an entity. An integral component in the recovery process is the availability of disaster recovery documents and files. In addition, periodic testing of the recovery alternatives determines their effectiveness as well as proves an opportunity to make adjustments to the recovery process before a disaster occurs.

DIAMOND STATE PORT CORPORATION  
SCHEDULE OF FINDINGS AND RESPONSES  
FOR THE YEAR ENDED JUNE 30, 2007  
(Continued)

**Condition:**

An Information Technology (“IT”) Disaster Recovery Plan is a written plan for an IT operation to be restored following a disaster. A disaster, in this context, is defined as an event which destroys the IT processing environment (“Data Center”). Although the IT Department is able to recover quickly from certain data loss events, the Port also needs a full disaster recovery plan which includes a provision for an off-site back-up facility.

A Business Continuity Plan is a broader plan to assure that Port operations continue in the event of a disaster. It includes planning for a comprehensive array of manual and automated activities. The IT Disaster Recovery Plan is a part of a Business Continuity Plan.

**Cause of Condition:**

Current data backup facilities are on-site in a Port warehouse and currently there is no IT Disaster Recovery Plan and Business Continuity Plan.

**Effect of Condition:**

In the current situation the data processing function and the operating departments could not continue to operate should the Port suffer catastrophic loss from a disaster.

**Recommendations:**

We recommend that the Port draft an IT Disaster Recovery Plan and Business Continuity Plan. When the IT Disaster Recovery Plan is completed, the IT Department management begin to take the necessary actions in order to ensure that the backup Data Center is operational as soon as possible. We also recommend that, once the backup Data Center is fully operational, a disaster recovery test be performed, at least annually, and the results of the test be documented in a report and distributed to the applicable Port departments. In addition, we recommend that the IT Disaster Recovery Plan should be updated annually.

DIAMOND STATE PORT CORPORATION  
SCHEDULE OF FINDINGS AND RESPONSES  
FOR THE YEAR ENDED JUNE 30, 2007  
(Continued)

We recommend that, as part of the development of the operating departments' Business Continuity Plans, Port management ensure that the Plans to include, at the minimum, the following:

- Designation of the alternate operating department site.
- Document files retention and storage.
- List of the Recovery Team's members.
- The procedures that will be followed by the operating department in the event of a disaster, which should include the individual responsible for declaring a disaster situation and assembling the Recovery Team.
- Emergency Personnel Contact List
- Service Vendor Contact List
- Employee Phone List
- Inventory of computer hardware and software used by the operating department.
- List of the required computer supplies and department forms that are stored at the alternate operating department site.

Also, at least annually, the operating departments' Business Continuity Plans should be updated and tested to ensure that they will work when needed.

**Costs and Benefits of Recommended Action:**

Costs include the cost of an off-site data backup facility and the time needed to develop and test the IT Disaster Recovery Plan and Business Continuity Plan. The benefit is that the Port would be prepared to deal with a disaster and resume operations much more quickly with an IT Disaster Recovery Plan and Business Continuity Plan.

**Client Response:**

On August 10, 2007, Inigo Thomas, IT Director, discussed disaster recovery and notified us that he will discuss with Port and DEMA management the possibility of arranging an off site backup Data Center.